Windows 7 Testing

Steve Slight

CIO Council Meeting
July 13, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Windows 7 Discussion

- Windows 7 testing
  - Agency proposed schedules are being forwarded via CAMs and AOMs
  - Scheduled two months for testing
  - How ready are your agency applications for Windows 7?
  - What help, if any, are you considering for remediation?

- Windows 7 communications
  - Are we communicating enough?
  - How should we tie in the ISOs?
  - Do you want to be included in the technical issues communications?

- Windows 7 implementation planning
  - Plan to work with the PC refresh schedule
  - Can we segregate agency departments during deployment if required?

Security Update

Trey Stevens

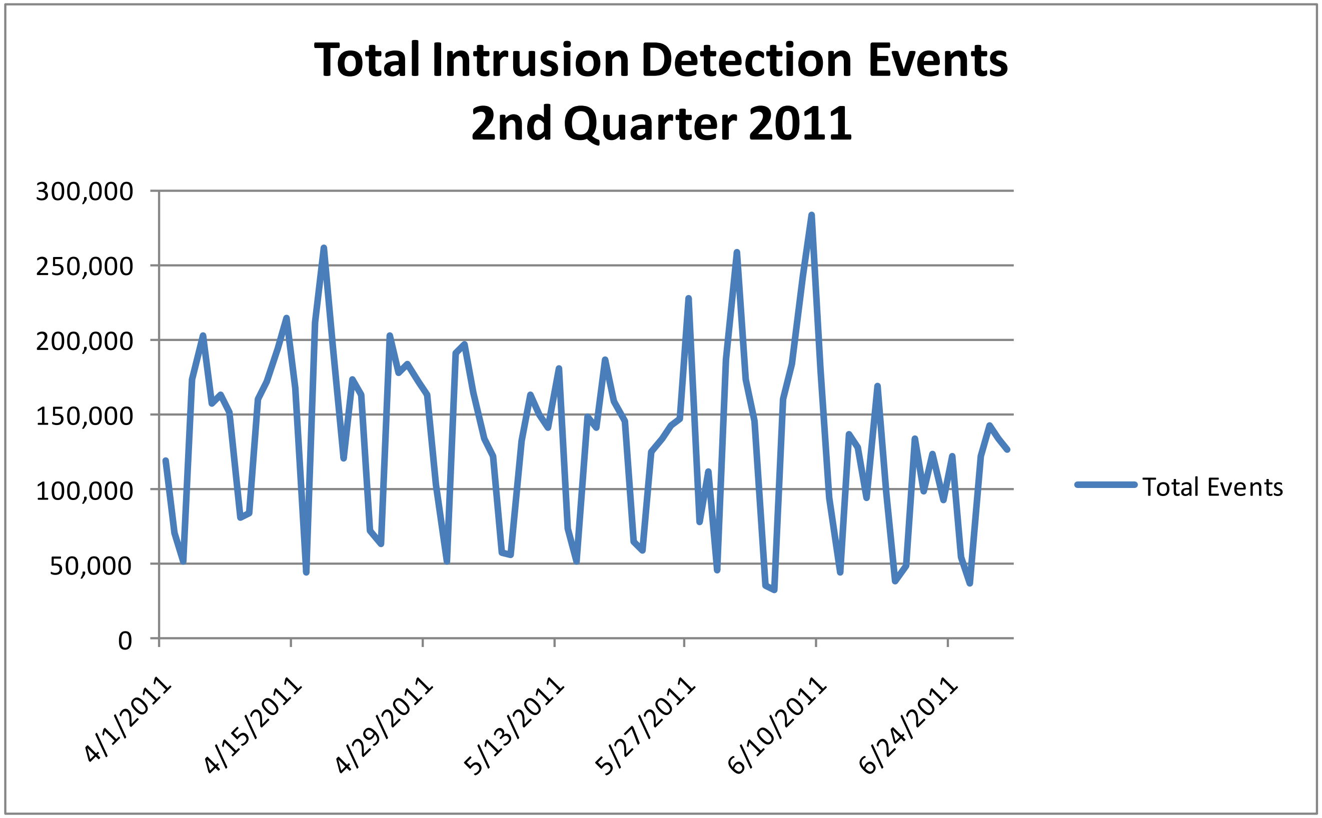
CIO Council Meeting
July 13, 2011

IT INFRASTRUCTURE PARTNERSHIP

VITA

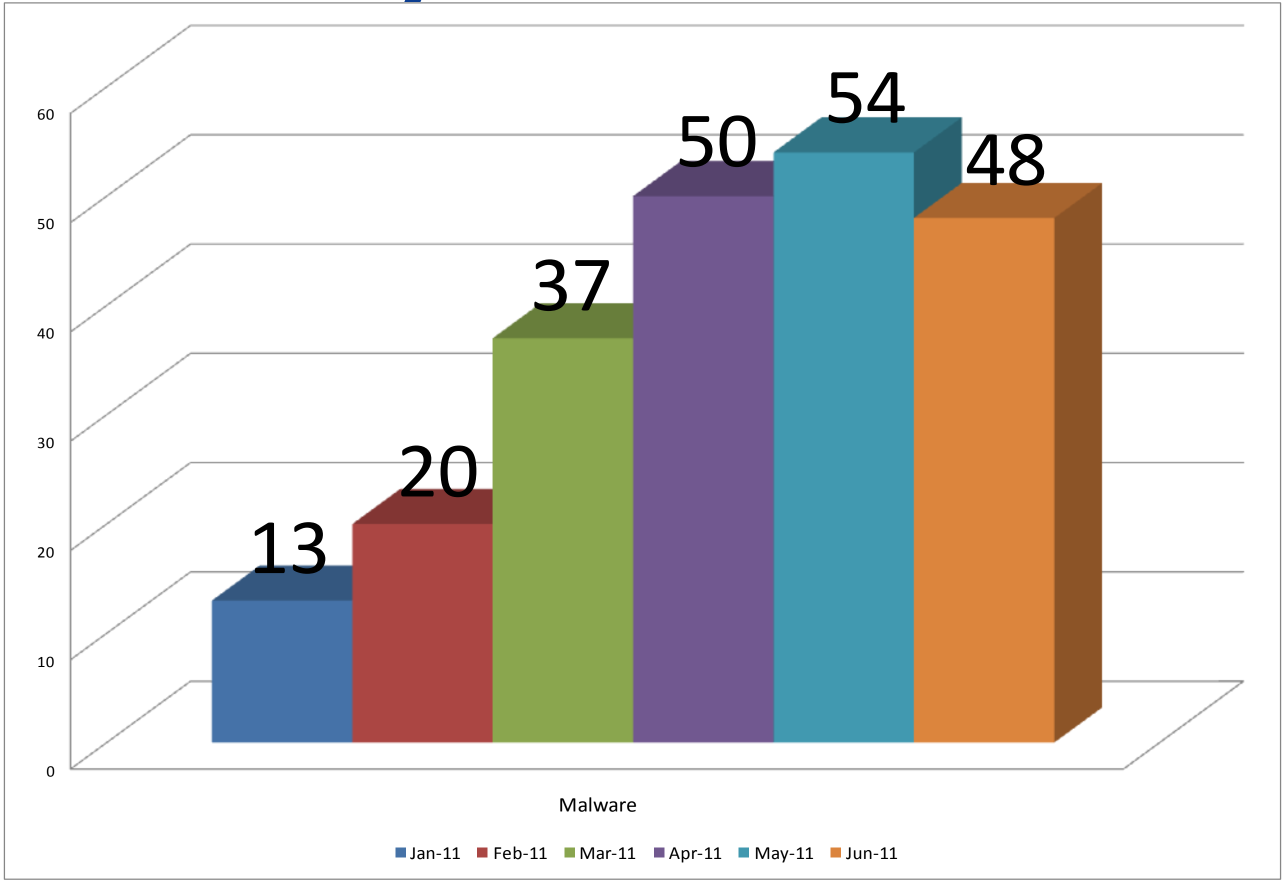
NORTHROP GRUMMAN

Security Intrusion Detection



During the second quarter of 2011 there were 12,187,705 potential attacks seen across all network and host-based intrusion sensors.

Security Incident Trend



- The number of malware-related incidents more than doubled from the first quarter
- Malware is using vulnerabilities in Java JRE, Adobe Acrobat Reader and Adobe Flash

Java and Malware

- While Adobe Acrobat Reader and Flash are patched by the IT Partnership, Java JRE is not.
- Java JRE is currently installed on 38,408 unique devices on the COV network.
- These devices are running a total of 96 different versions and almost 40 percent (15,343) have multiple versions of Java installed.
- Antivirus products only are effectively detecting and cleaning 50 percent of the variants being found. The malware is starting to exhibit more malicious behavior.
    - ➢ Outbound network communication attempts
    - ➢ Rootkit behavior
    - ➢ Keystroke logging
    - ➢ Data compromise attempts

Add Java to core software?

- Must remediate vulnerability
- Recommend updating to the latest version - JRE 1.6_update 26

Pro

- Standardize patching, executed by ITP
- Centralized reporting
- Patch testing driven by ITP

Con

- Some applications written in Java are written to a specific version
- Patch testing driven by ITP

How should we proceed?